

# Virtual Servers

## Service Description

Virtual Servers provide a virtualized server environment with enhanced security for hosting business applications in the State Data Center. The virtual server environment supports Microsoft Windows Server and Red Hat Enterprise Linux Server operating systems. Virtual machines (VMs) can be sized to support customer processing requirements via a fixed incremental configuration of memory, processor and disk space (see Service Notes section for configuration details).

1. **Virtual Machine (VM):** This offering provides for a centrally provisioned and patched VM operating system (OS) and related system utilities. This offering includes two core processors, 4GB RAM and 80GB OS file storage. Admin will enable provisioning of a vendor-supported version of Microsoft Windows Server Operating System or a vendor-supported version of Red Hat Enterprise Linux Server Operating System. Admin will manage and maintain the Virtual Server OS, including basic operating system testing and installation of service packs and patches, to ensure the operating system patches do not materially impact the core server performance.
2. **Virtual Machine (VM) – Legacy Isolation:** If an agency is unable to use a vendor-supported server operating system, Admin will assign the VM Legacy Isolation service offering to the agency. These VMs are hosted on isolated infrastructure and are configured to help mitigate security risks, and the server operating system is supported by the agency. Admin will determine an agency's need for this service offering on an exception basis; this offering is not orderable by agencies.

## Service Notes\*

- Full agency server migrations to the State Data Center are not included in this service. This service is focused on the provision and support of a new virtual server instance.
- The virtual server environment is based on VMware ESXi.
- Servers will be charged from the time they are provisioned until they are de-provisioned.
- Storage for customer data is available through the [Enterprise Storage](#) service.

***\*See Service Detail for additional important Service Notes and Customer Responsibilities.***

## Customer Benefits

- **Cost savings** – Customers do not have to invest in server hardware, server OS licenses, data center facilities and personnel.
- **Efficiency** – Sharing common equipment and resources allows for more cost-efficient operations and support.
- **Security** – Robust policies, controls and systems are designed to enhance security.
- **Scalability** – VM configurations can be modified within the existing footprint of the VM cluster as business needs change.
- **Support** – Monitoring and response by trained Admin technical staff ensures maximum utilization and minimum server downtime.

## Service Rates

Service Offering	Cost per Month
Virtual Machine (VM)	Contact ARM
Virtual Machine (VM) – Legacy Isolation*	Varies by system

\*Note: This offering is not orderable by agencies, and may only be assigned by Admin on an exception basis. See Additional Service Notes for more detail.

## Virtual Servers – Service Detail

### This Admin service includes:

#### ***Facilities Management***

- Management and monitoring of physical security to data center.
- Management and monitoring of the data center environment (e.g., racks, power and cooling).

#### ***ESXi Host Systems Engineering***

- Provisioning and set-up of ESXi host server hardware and software in accordance with Admin standards and policies.
- Hardware and software enhancements to the ESXi host server over time.
- Upgrades of ESXi host service components.

#### ***ESXi Host Systems Maintenance***

- Administration and maintenance of hardware to ensure that each ESXi host server is reliable, is performing adequately and is providing overall service availability.
  - Maintain ESXi host server hardware and software at recommended patch and release levels following standard change management procedures.
  - Standard capacity and performance analysis reporting capabilities for customers to review utilization, performance and trending information for processors and memory.
- Admin provides and maintains a VM OS and related systems utilities.
  - Admin installs manufacturer field change orders, service packs, firmware and software maintenance releases.
  - Admin performs product patch, “bug fix,” service pack installation or upgrades to the current installed version.
- Admin manages and maintains (e.g., procure, monitor, track status, verify, audit, perform contract compliance, renew, reassign) software licenses and media.

#### ***ESXi Host Systems Support and Monitoring***

- Responsive support to incidents.
- Responsive support to unscheduled service outages in a timely manner.
- Provision of diagnostic information to assist with customer application support needs.
- Repair or replacement of failing hardware components.
- Ongoing security monitoring and management.

- Security event monitoring, detection and notification.
- Periodic vulnerability scanning and reporting.
- Security event/vulnerability remediation.
- 24/7 access to the DTO Service Desk.
- Best effort prioritized on-call “after hours support.”
- Simple Network Management Protocol (SNMP) and Internet Control Message Protocol (ICMP) based monitoring and alerting.
- Hardened server images.
- System management and reporting software.
- Monitoring and alerting services to ensure operating system is up and operating normally.

### ***Network Connectivity***

- Connectivity within the data center to a dedicated department Virtual Local Area Network (VLAN) to keep data and applications separated from other department data and applications.

### ***Virtual Machine Redundancy in State Data Center***

- The VMs are configured with full redundancy allowing system recovery within the same data center.
  - In the event that a physical server fails, also commonly referred to as an ESXi host hardware failure, the automated high availability feature is invoked. All VMs affected by the ESXi hardware failure are migrated to an alternate ESXi host and re-started on the alternate host within the virtualization cluster.
  - All workloads are supported with minimal impact to performance with unplanned downtime related to the VM migration and the restarting of the VM on an alternate host in the virtualization cluster. The alignment and compliance of application requirements are maintained as when the VM was initially provisioned.
    - Server failover (VMware HA) capabilities do not support application level load balancing at this time.
    - Additional disaster recovery capabilities are under development.

### ***Virtual Machine Backup***

- Backup of VM OS, system utilities, applications and VM configurations.

## **Related Services**

A Virtual Server Hosting customer might also be interested in these Admin services which are offered separately:

- Database Hosting
- Enterprise Storage
- Data Backup

## Service Level Objectives

### ***Service Level Targets***

TBD

## Additional Service Notes

- **Virtual Machine (VM)**
  - Admin will ensure the agency has remote access to the virtual server. Agencies will be responsible for purchasing client remote access licenses (e.g., two-factor authentication from Juniper and/or Citrix) for remote access.
  - Admin will coordinate with the agency for any planned Admin changes or outages that will affect the agency's server environment.
  - Requests for installations, adds, moves or change that exceed 40 hours will require additional funding. Admin will provide an estimate before beginning work.
  - Agencies are expected to maintain their VM hosted operating systems at vendor supported versions in order to get the most benefit from this service. A list of currently supported server operating systems is available from Admin.
  - If a customer's business applications require a larger server environment or a custom configuration, please contact Admin to investigate an alternative, custom configuration.
  - The standard patching maintenance window is Saturday from 8 a.m.-noon. Patches are applied 10 days after release. Patches are occasionally applied sooner based on the risk of the unpatched vulnerability.
  - VM OS are subject to security scanning services by DIS prior to being placed into production.
- **Virtual Machine (VM) – Legacy Isolation**
  - This environment may result in reduced application functionality in order to mitigate security risks inherent in the legacy server operating system software environment.
  - This offering will have reduced support (e.g., patching is no longer available). This offering is primarily focused on protecting the broader Admin application and infrastructure environment from security risk introduced by hosting legacy server operating system software.
  - The environment is composed of dedicated hardware and software components with advanced security configurations. The costs of these components and the associated labor are included in the service offering rate. Examples of additional security associated with this offering include, but are not limited to: separated VLAN, restricted user access, additional firewalls to isolate the legacy server operating system from the mainstream network, etc.
  - The agency is responsible for initial provisioning, configuration, patching and ongoing management of the VM OS.

## Customer vs. Admin Responsibilities

This section identifies in detail Admin and customer responsibilities for each service offering.

Responsibilities	Admin	Customer
<b>Data Center Facilities</b>		
Data Center power, cooling and related support infrastructure.	X	
Data Center network infrastructure.	X	
Data Center facilities security.	X	
Data Center facility structure maintenance and enhancements.	X	
<b>Hardware</b>		
ESXi host server hardware (processor, memory, storage for system files) at the State Data Center.	X	
ESXi host server hardware (processor, memory, storage for system files) at disaster recovery site (Clemson University data center).	X	
Virtualization software (hypervisor and virtualization management tools).	X	
<b>Standard System Software</b>		
VM server operating system.	X	
Standard security software (anti-virus, host intrusion detection, scanning) for VMs.	X	
Standard system management tools.	X	
Server remote access software (Citrix or Juniper).	X	
Client remote access software (Citrix or Juniper).		X
<b>Non-Standard System Software</b>		
Additional VM OS CALs.		X
Non-standard system management tools.		X
Non-standard security software.		X
<b>Application Software</b>		
Custom developed.		X
Commercially provided.		X
Middleware/utility software.		X
Other software not defined above.		X
<b>Initial Provisioning and Configuration Management of:</b>		
ESXi host server hardware/software.	X	
Virtual machine instance.	X	
VM OS and utilities.	X	
Non-standard system software.		X
Applications and database software.		X
<b>Patching and Lifecycle Configuration Management of:</b>		
ESXi host server hardware/software.	X	
VM OS and utilities.	X	

<b>Responsibilities</b>	<b>Admin</b>	<b>Customer</b>
Non-standard system software.		X
Applications and database software.		X
<b>Monitoring and Fault Management – Fault Monitoring and Event Notification/Triage, Recovery and Troubleshooting (perform diagnostics, maintenance and break/fix support)</b>		
ESXi host server hardware/software.	X	
Virtual machine instance.	X	
Virtual machine fail over instance (base disaster recovery capabilities).	X	
VM OS and utilities.	X	
Non-standard system software.		X
Applications and database software.		X
<b>Capacity and Performance Management</b>		
Implement and maintain tools for performance/capacity planning.	X	
Provide reporting for system performance and utilization.	X	
Monitor usage to proactively identify capacity or performance issues.	X	
Evaluate, identify and recommend changes to enhance performance.	X	
<b>Security Monitoring and Management</b>		
Anti-virus system management and scanning of the VM environment.	X	
Security event monitoring, detection and notification.	X	
Periodic vulnerability scanning and reporting.	X	
Security event/vulnerability remediation.	X	X
ESXi host server hardware and software.	X	
VMsSystem utilities software.	X	

All services are delivered in compliance with State of South Carolina Information Security policies, as presented in SCDIS-200.